(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
14 June 2001 (14.06.2001)

PCT

(10) International Publication Number
WO 01/43338 A1

(51) International Patent Classification[7]: H04L 9/08

(21) International Application Number: PCT/CA99/01164

(22) International Filing Date: 9 December 1999 (09.12.1999)

(25) Filing Language: English

(26) Publication Language: English

(71) Applicant *(for all designated States except US)*: **MILLINX BUSINESS GROUP INC.** [US/US]; 3226, 1001 Fourth Avenue, Seattle, Washington 98154 (US).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **WILLIAMS, Donald, Lloyd** [CA/CA]; 3057 McBride Avenue, Surrey, British Columbia V4A 3G9 (CA). **BAZARGAN, Ali, Reza** [CA/CA]; 15475 Goggs Avenue, White Rock, British Columbia V4B 2N5 (CA).

(74) Agent: **SMITH, Paul**; Paul Smith Intellectual Property Law, 330 - 1508 West Broadway, Vancouver, British Columbia V6J 1W8 (CA).

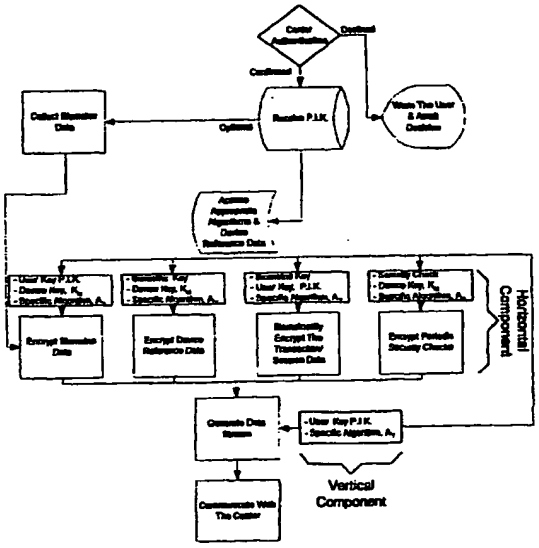
(81) Designated States *(national)*: AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, DM, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published:
— *With international search report.*

[Continued on next page]

(54) Title: METHOD AND APPARATUS FOR SECURE E-COMMERCE TRANSACTIONS



(57) Abstract: A method of authenticating the identity of a user of a communication device and providing a securely encrypted communication channel, comprises first authenticating the identity of the user using biometric information collected and encrypted using apparatus which interfaces with a communication device. After authentication is complete the communication is encrypted using a series of different algorithms which include an encryption key derived from the user's biometric data as well as device-specific algorithms broadcast from time to time to the device, and an algorithm programmed into the device. The encrypted data packets include several separately encrypted components, the arrangement of which varies in successive data packets. The invention provides a means for securely authenticating the identity of a user without requiring the use of any particular communication device in order to do so.

WO 01/43338 A1

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

TITLE OF THE INVENTION

METHOD AND APPARATUS FOR SECURE E-COMMERCE TRANSACTIONS

FIELD OF THE INVENTION

This invention relates to the encryption of data and the authentication of the identity of participants in electronic commerce transactions and communications. In particular this invention relates to methods for authenticating the identity of participants and for securely encrypting said transactions and communications and apparatus therefor.

BACKGROUND OF THE INVENTION

The authentication of the identity of participants is a key requirement of most electronic commerce transactions. The security of the information being transmitted is also a concern, particularly where such information represents confidential data of the participant.

It is known in the prior art to provide authentication of a participant by collecting and verifying the participant's biometric data. It is also known to encrypt the biometric data when transmitting it for authentication purposes.

U.S. Patent No. 5,872,834 to Teitlebaum discloses a system involving a biometric input sensor to capture biometric data that is then encrypted and transmitted. The patent notes that the system is useful in electronic commerce applications to authorize payments, in billing applications, for credit authorization and for other electronic commerce purposes. The patent discusses the use of biometric input devices associated with

telephones or cellular telephones. An authentication center may be used to provide third party authentication. Teitlebaum points out that such a system enables reliable identification of the user of a communication device without being dependent on that particular communication device.

U.S. Patent 5,956,409 to Chan et al. describes a method for the secure application of seals. An optical image of a seal is recorded by a computer and encrypted using a key for encryption generated in response to template biometric data from authorized persons. When a person seeks to use the seal, for example to apply the seal to a document, test biometric data is input from that person and used to generate a key for decryption. If the test biometric data matches the template biometric data, the key for decryption will be useful for decrypting the encrypted seal, and the person seeking access to the seal. The test biometric data represents a handwritten signature given contemporaneously by the person seeking access, and is verified against a set of template signatures earlier given by at least one authorized person. Specific signature features are determined in response to the template signatures and used for generating one or more keys for encrypting the seal. Similarly, specific signature features are determined in response to the test signature and used for generating keys for decrypting the seal.

The use of more than one type of biometric parameter to more reliably identify individuals is well known. US Patent No. 5,412,738 to Brunelli et al., US Patent No. 5,719,950 to Osten et al. and US Patent No. 5,930,804 to Yu et al. each discuss the use of at least two biometric features to authenticate the identify of a speaker. Yu et al. further discuss means to prevent biometric data forgery by sensing the temperature of the user's finger when capturing fingerprint data.

The use of dynamic encryption keys which are periodically downloaded to an encryption device and further using keys permanently stored in the device is also known.

U.S. Patent No. 4,944,006 to Citta et al. describes a secure data packet transmission system and method which includes a head-end having a software implemented 16 bit shift register which encrypts a bit packet. Dynamic encryption is provided by utilizing an initial preset for the software corresponding to a preset

encryption key for the shift register. Authorized subscriber terminals are provided with memories and decryption keys are downloaded. The bit packets are assembled with a global bit packet encrypted with a global encryption key and subsequent individually addressed bit packets encrypted with address keys. The address keys and terminal addresses are permanently stored in the subscriber terminal memories. The global encryption keys are changed periodically. Means are provided in each subscriber terminal for storing a number of global decryption keys, which are cycled through in attempts to decrypt the global packets. One of the global decryption keys is a permanent default key associated with the subscriber terminal to assure that communication with that terminal is possible despite a lack of knowledge of the terminal address or the other global decryption keys in its memory.

U.S. Patent 5,805,705 to Gray et al. discloses a system for synchronizing encryption/decryption keys in a data communication network. The keys are changed periodically at the source and destination nodes for an established connection. A destination node must know not only the value of any new key but also when to begin using that key to decrypt received data packets. Synchronization (making sure a data packet is decrypted using a decryption key correlated with the encryption key used to encrypt the same packet) is achieved by defining a single bit in each packet header as a key synchronization bit. As long as key synchronization bit value remains unchanged from one received packet to the next, a receiving node will continue to use the same decryption key it has been using. When a change in the key synchronization bit value is detected, the receiving node will begin using a previously received, new decryption key.

U.S. Patent 5,887,065 to Audebert describes a system and method for user authentication having clock synchronization. The system includes a first unit adapted to communicate with a second unit. The second unit grants conditional access to a function or service in accordance with an authentication operation. Both units are capable of running software for generating passwords by means of encryption of several dynamic variables as for example a time dependent variable and/or a variable representing the number of formulated authentication requests. The encryption may be performed using a dynamic key.

U.S. Patent 5,937,068 to Audebert describes a system and method for user authentication employing dynamic encryption variables. The system includes a first card-like unit adapted to communicate with a second unit giving only conditionally access to a function. Both units are capable of running software for generating a password by means of encryption of a plurality of dynamic variables produced separately but in concert (so as to have a predetermined relationship, such as identity, with one another) in the units. The encryption is carried out in each unit by a public algorithm using a dynamically varying encryption key. Each time an access request is issued by a card user, the key is modified as a function of the number of access requests previously formulated by the card user.

It is an object of this invention to provide a secure means of conducting electronic commerce transactions and other communications wherein authentication of participants is highly reliable.

It is a further object of this invention to provide a secure means of conducting electronic commerce transactions and other communications, wherein reliable participant authentication may be achieved regardless of the specific communication device being used by a participant.

It is yet a further object of this invention to provide a high degree of inherent encryption security.

It is a further object of the invention to incorporate biometric data in the encryption process in a manner that minimizes the effective use of biometric forgery.

These and other objects of the invention will be better understood by reference to the following disclosure.

SUMMARY OF THE INVENTION

The invention provides a means for securely authenticating the identity of a user without requiring the use of any particular communication device in order to do so.

A user's biometric data is retained in a database at an authentication center. A number of biometric encryption devices are also enabled for use with the secure system. A registered user may use any biometric encryption device enabled by the system to establish a secure communication. The biometric encryption device may be used in association with a variety of standard communication devices.

When a user wishes to authenticate his or her identity, for example in connection with an electronic commerce transaction, the user's biometric data is collected by and transmitted in encrypted form to the authentication center. This phase is known as the initial authentication phase.

After the user's identity has been authenticated, the user's biometric data continues to be used as an integral component of the encryption process itself during the secure session phase of the communication.

In the initial authentication phase, the user's biometric data is encrypted using a combination of a device-specific encryption key programmed into the device as well as a time-specific encryption key broadcast from time to time from the authentication center to the device.

In the secure session phase of the communication, session information is transmitted in composite data packets comprising varying sequences of encrypted session data, encrypted biometric data and encrypted device-specific reference data. Each of the components is encrypted using different keys and all components are encrypted using a sequence of different encryption time-specific algorithms which have been previously broadcast from the authentication center to the device. The relative positions of the components in the data packets are also changed throughout the transmission.

The various aspects of the invention will be more specifically appreciated by reference to the following detailed description of the preferred embodiment and by reference to the claims.

BRIEF DESCRIPTION OF THE DRAWINGS

The preferred embodiment of the invention will be described by reference to the drawings in which:

Fig. 1 is a diagram showing participants in a typical electronic commerce transaction according to the invention;

Fig. 2 is a block diagram illustrating the principal operational components of a biometric encryption device according to the invention;

Fig. 3 is a diagram illustrating the downloading of default keys and algorithms and a schedule therefor;

Fig. 4 is a flowchart of the steps in the initial authentication phase from the point of view of the biometric encryption device according to the invention;

Fig. 5 is a diagrammatic representation of the structure of a transmission packet from the device in the initial authentication phase;

Fig. 6 is a general flowchart of the steps in the initial authentication phase from the point of view of the authentication center;

Fig. 7 is a general flowchart of the steps in the secure mode phase from the point of view of the biometric encryption device;

Fig. 8 is a general flowchart of the steps in the secure mode phase from the point of view of the authentication center; and,

Fig. 9 is a diagrammatic representation of the transmission packet structure in the secure mode according to the invention.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENT

Fig. 1 illustrates the principal elements of a secure communication according to the invention. In the illustrated example, a first participant P1 desires to conduct a secure electronic commerce transaction with a second participant P2. For example, participant P2 may be a bank and participant P1 may be a consumer who wishes to have bank P2 transfer funds to a third party (not shown) to complete the consumer's purchase of product from the third party using a point of sale device.

The transaction is conducted by means of communication devices 10 and 12 which may be any form of communication device. In the illustrated example, the device is a telephone, but in other cases it may be a cellular phone, PDA, radio, modem or other communication device. Communication may involve any communication medium such as the Internet, one or more public switched telephone networks, a private network, etc.

Participants P1 and P2 may have their identities authenticated and their transmissions encrypted by means of biometric encryption devices 14, 16 according to the invention.

When participant P1 wishes to establish secure communication with participant P2, communication is enabled between device 14 and communication device 10.

In one embodiment, communication is then established between communication device 10 and communication device 12 which is associated with participant P2. Once communication between P1 and P2 is established, one or both of P1 and P2 will formulate a request for secure communication facilities and will transmit the request to authentication center 20. Authentication center 20 will open a communication channel to each of P1 and P2 and will proceed to verify the identity of P1 and P2 in accordance with the method of the invention described below. Assuming the identities of P1 and P2 are verified, authentication center 20 authorizes the establishment of a secure channel between P1 and P2, with authentication center 20 acting as a go-between for the secure communication session.

In another embodiment, P1 first establishes communication with authentication center 20 and undergoes authentication of P1's identity. Authentication center 20 then receives P1's request for secure communication with P2. Authentication center 20 then communicates with P2, verifies P2's identity, and authorizes a secure channel between P1 and P2, with authentication center again acting as a go-between.

In yet another embodiment, the authentication center may simply authenticate the identity of a participant and transmit a message to a third party confirming the authentication.

Participant and device registration

According to the invention, participants in the system are pre-registered with authentication center 20. In the registration process, the participant provides samples of the participant's unique biometric traits, as well as a participant-selected passphrase. A PIN number may also be provided depending on the level of security desired. However the preferred embodiment described herein does not rely on use of a PIN number.

The user-supplied passphrase is used by the center to derive an encryption key known as the personal identification key (PIK). The PIK is used in the encryption process as described below.

Some registered participants may elect to obtain a biometric encryption device which may be portable or intended to be permanently retrofitted into an existing communication device. In the event that a new participant owns a communication device that has built-in biometric encryption device according to the invention, such device can be enabled upon registration of the participant.

Biometric encryption devices can also be registered or enabled independently of the registration of participants. At the time of registration or enablement of biometric encryption devices, the center will provide the device with device-specific reference data for eventual use in conducting secure communication.

Biometric Encryption Device

Biometric encryption device 14 may take a variety of different forms including:

- a stand alone unit, such as a point of sale device which may be selectively associated with a communications device

- an integral sub-assembly of a communication device

- a portable plug-in (e.g. into a PC Card slot) for a communication enabled device

- a retrofittable component to an existing communication device, such as a replacement handset for a telephone

- a chip embedded in the communication device which provides the processing, encryption/decryption and memory functions, and which is used in conjunction with biometric input sensors associated with a communication device.

Fig. 2 illustrates the principal functional elements of biometric encryption device 14 according to the invention.

Memory means 22 stores encryption keys and algorithms as well as key and algorithm scheduling information as described in more detail below. Memory 22 includes at least one device-specific key (K_M) and at least one device-specific algorithm (A_M) for use in encryption as described below. K_M and A_M are known to the center 20.

Clock 24 is used to determine the precise time at which a request for authentication will be dispatched for the purposes of selecting the appropriate time-dependent key (K_B) and algorithm (A_B) to be used to encrypt the request and related data. The time-dependent key and algorithm K_B and A_B are discussed below.

Biometric input sensors 26 comprises means for capturing biometric data, for example fingerprints, pulse data and voice print. It also analyzes the raw biometric data to extract features which uniquely characterize an individual user, and converts the

extracted features into a format which is consistent with the authentication center's protocol for such data.

Encryption/decryption engine 28 operates to encrypt and decrypt messages or data according to encryption keys and algorithms stored in memory 22.

A communications manager 30 provides an interface for inputs to the device 14 and for outputs from device 14 either directly to a communication channel or to the communication device for transmission by the communication device. It will be appreciated that the physical form of the interface take a variety of forms including a port connecting to a communication device port, a hard wired connection in the case of a biometric encryption device which is built into a communication device, or other suitable interface means. Inputs to device 14 include notably data to be encrypted, information downloaded from time to time from authentication center 20 such as encryption keys, algorithms and algorithm sequencing and scheduling information (described below), and participant data required for the authentication process such as participant's name, identification of the other participant, etc. Communications manager 30 may also act to monitor the communication otherwise being conducted through the communication device so as to divert and encrypt only a limited selection of information, such as a credit authorization or funds transfer request, as opposed to encrypting an entire communication session.

User interface 32 may comprise any suitable user interface means enabling device 14 and the user to exchange instructions and responses. It will be appreciated that depending on the selection of the type of biometric inputs to be used in the authentication process, and the functionality which the biometric input sensor 26 is given, some or all of the user interface functions or the data input functions may be provided by biometric input sensor 26 itself.

A CPU 34 coordinates the various functions of the device.

Broadcast Keys, Algorithms, Sequences and Schedules

From time to time, authentication center 20 transmits to biometric encryption device 14 updated encryption keys, algorithms, an algorithm sequence and a schedule for their use. Such updated information is stored in device memory 22. The updated information is broadcast to all enabled devices at unpredictable times. This process is illustrated in Fig. 3 wherein A_B, K_B and S_B are algorithms, keys and sequences and schedules specific to groups of biometric encryption devices or to individual devices. Such grouping may be preferred to minimize the time required to broadcast the information compared to broadcasting such information for each individual device in use in the system. However, the use of different keys, algorithms and sequences and schedules for at least different groups of devices minimizes the possibility of unauthorized interception.

In addition, any time a user powers up a communication device associated with an enabled biometric encryption device 14, contact with the authentication center 20 is made and current keys, algorithms and sequences and schedules applicable to that device are retrieved from the authentication center. Preferably such transmission from the authentication center comprises a bundle of keys, algorithms and schedules such that a person obtaining possession of the device 14 and monitoring the update will not be able to easily determine which of them are intended for the specific device.

The broadcast keys, algorithms and sequences and schedules A_B, K_B and S_B are stored in memory 22 for later use in the initial authentication phase of a secure communication.

Initial Authentication Phase

Fig. 4 is a flowchart of the initial step in establishing a secure communication to cover the transaction. In this phase of the process initial authentication of the

participant/user is performed. The device 14 prompts the user to enter his or her name. The user is then prompted (40) to input biometric data. Such biometric data may comprise any number of biometric traits, but the preferred embodiment of the invention captures biometric data for at least two traits to maximize the reliability of the authentication and to render the process relatively more independent of the use of specific communication devices. The biometric data is read (42) by sensor 26 which then extracts (44) the distinctive features from the raw biometric data and formats (46) them according to the biometric data formatting protocol used by the authentication center 20.

In order to effect encryption, CPU 34 first determines (48) the current time by reference to clock 24.

CPU 34 then retrieves (50) S_B from memory 22 (S_B was previously received from authentication center 20 in a broadcast or at powering up of the communication device as described above). S_B determines which specific key and algorithm are to be used for communications initiated at the specific time determined by reference to clock 24 and these are retrieved (52). The time-specific key and algorithm are designated as K_T and A_T.

A_M and K_M are also retrieved (54)).

A_T and A_M are then combined (56) to form a device-specific encryption algorithm, while K_T and K_M are combined to form a device-specific encryption key. The resulting algorithm and key are therefore unique to that particular device at that particular time. They are then delivered (58) to the encryption/decryption engine 28.

The biometric features which have previously (46) been formatted according to the required biometric data formatting protocol are then encrypted (60) by the encryption/decryption engine 28. Similarly the engine 28 encrypts (64) the user's name.

A device-specific permanent ID number is then retrieved (66) from memory 22 and is encrypted using A_T and K_T only.

A transmission packet for requesting initial authentication is then formulated (66) comprising:

- the encrypted biometric information
- the encrypted user name
- an encrypted device-specific ID number

The device-specific ID number is encrypted only at a system level since the authentication center 20 must be able to identify the alleged identity of the biometric encryption device 14 in order to know how to formulate a decryption key and algorithm. Thus the device ID is encrypted according to an encryption algorithm and key which are common to all devices within the system and that are of the same type (e.g. a portable biometric encryption device, a device permanently associated with a cellular telephone, etc.). Such encryption may for example be done using device-type specific A_T and K_T.

Once the device is identified, the authentication center formulates the decryption key and algorithm using the same information used to encrypt the data in device 14, all such information having been either broadcast from the center 20 itself, including A_B (and therefore A_T), and K_B (and therefore K_T), or are known to the center at the outset (A_M and K_M). Once the message is decrypted, the biometric data is compared to that stored by authentication center 20 for verification.

Verification is then communicated (70) by center 20 to device 14 and secure mode communication is enabled (78). The verification message transmitted from center 20 to device 14 includes the personal identification key (PIK) of the user.

Secure Session Phase

In the secure session mode, the biometric data is used to create one or more biometrically derived encryption keys which are used to encrypt all or a portion of the transaction data or the communication itself as the case may be. The use of an encryption key derived from the user's biometric data ensures a high level of security for the transaction or communication and a high level of confidence in the identity of the user.

The risk of biometric data forgery is minimized by combining biometrically derived encryption with encryption parameters which include device dependent parameters, broadcast dependent parameters and dynamic varying of not only the keys and algorithms involved, but of the structure of the transmission packets themselves.

Throughout the secure session, further biometric data may be collected from time to time to periodically authenticate the identity of the user and to avoid interception and overriding of an on-going communication.

The components of a transmission packet in the secure mode are:

- encrypted biometric data
- encrypted transaction or communication data
- encrypted device reference data
- continuity check information

The packet may also include periodic security checks which are also encrypted.

Encrypted Biometric Data

This component of the transmission packet comprises the biometric data which has been collected from the user. In the preferred embodiment, such biometric data is

collected from time to time during the communication for the purpose of ensuring periodic authentication of the user. Each time a new collection is taken and transmitted, the authentication center re-authenticates the user's identity.

The biometric data portion of the transmission packet is encrypted using a key derived from a combination the device-specific key K_M and the personal identification key PIK.

Encrypted transaction or communication data

This comprises the electronic commerce transaction or financial data or the communication itself, as the case may be. This data is encrypted using a key derived from a combination of the user's biometric information and the personal identification key PIK.

Thus it will be appreciated that the transaction or communication data is encrypted in a highly secure and user-specific manner in that the user's unique biometric data is used as a part of the encryption key. In addition, the incorporation of the user's personal identification key PIK (which was derived from the passphrase selected by the user and which is known only to the center 20) minimizes the risk of successful interception of the communication.

Encrypted device reference data

This comprises device specific data (e.g. a page of text or images) which is programmed into the device 14 at the time of registration and which is known to the center 20. While this reference data may be changed from time to time, in the preferred embodiment it remains the same for the course of a given secure communication.

The key used to encrypt the device reference data is derived from a combination of the biometric data of the user and the device-specific key K_M.

Algorithm

The algorithm used to encrypt the packets changes or rotates throughout the transmission as algorithm-1, algorithm-2 ... algorithm-n. In the preferred embodiment the number of packets which have been transmitted determines each transition from one algorithm to the next. In Fig. 9 the sequence of successive packets and the algorithms used to encrypt their components is shown in the horizontal dimension.

The algorithms and their sequence are included as part of the broadcast referred to above. Depending on the time at which a secure communication is enabled, a certain one of the broadcast algorithms will be used as the starting algorithm for the encryption of the secure mode communication. Successive algorithms may follow the sequence dictated by the broadcast.

Packet organization

The above identified components of a transmission packet, namely the encrypted biometric data, the encrypted transaction or communication data and the encrypted device reference data, are arranged in a given packet in a varying sequence. The sequence of types of data in a given packet is illustrated in the vertical dimension in Fig. 9. The sequence is a varying one which changes each time the algorithm changes (but which may change for any given algorithm as well).

The specific arrangements of types of data for each packet and/or for each algorithm are communicated to device 14 by the broadcast. Thus A_T is used to govern the arrangements. The key used for this purpose is the user specific key, PIK.

Thus is will be appreciated that the invention provides a highly encrypted communication which is a function of keys derived from the following sources:

- The biometric traits of the specific user
- The device itself (A_M, K_M)
- Arbitrary choice by the user (the PIK)
- The center (the device reference data)

The system according to the invention also provides device independence for a user. Although each device used is enabled for use with the system, a registered user may choose any enabled device to complete a transaction or communication. Such device independence gives the user flexibility in effecting secure transactions, and allows the system to track activity by a specific user, for example for billing purposes.

It will be appreciated that although the preferred embodiment of the invention has been described in relation to an electronic commerce transaction, the encryption method and apparatus may equally be applied to any communication, whether it is of a financial nature or not.

It will also be appreciated by those skilled in the art that while the preferred embodiment of the invention has been described in detail, variations to the preferred embodiment may be practised without thereby departing from the scope of the invention, which scope is reflected in the principles of operation and structure reflected in the foregoing disclosure and in the following claims.

CLAIMS

1. A method of authenticating the identity of a user of a communication device comprising the steps of:

determining the alleged identity of said user;

collecting biometric data from the user;

encrypting said biometric data;

delivering said encrypted biometric data to a communication device;

transmitting said encrypted biometric data to an authentication center; and,

comparing the biometric data to recorded biometric data for the user.

2. A method as in claim 1 wherein at least two types of biometric data are collected from the user.

3. A method as in claim 2 wherein one of said types comprises pulse data.

4. A method for authenticating the identity of a user of a communication device comprising the steps of:

providing apparatus having memory means, a biometric input sensor, an encryption engine and a communication interface for communicating information to said communication device;

operatively connecting said apparatus to said communication device by means of said interface;

requiring said user to input biometric data into said biometric input sensor;

using said apparatus to encrypt said biometric data; and,

using said communication device to dispatch said encrypted biometric data to an authentication center.

5. A method for authenticating the identity of a user of a communication device comprising the steps of:

providing apparatus having memory means, a biometric input sensor, an encryption engine and a communication interface for communicating information to said communication device, said apparatus being operatively connecting to said communication device by means of said interface;

requiring said user to input biometric data into said biometric input sensor;

using said apparatus to encrypt said biometric data; and,

using said communication device to dispatch said encrypted biometric data to an authentication center.

6. A method as in claim 5 further comprising the step of enabling said apparatus for biometric encryption through said authentication center.

7. A method as in claim 6 wherein said enabling step comprises further comprising the step of recording in said memory means encryption parameters supplied by said authentication center.

8. A method as in claim 7 wherein said encryption parameters are specific to said apparatus.

9. A method as in claim 8 wherein said encryption parameters comprise an encryption key and an encryption algorithm specific to said apparatus.

10. A method as in claim 7 or 8 wherein said encryption parameters comprise reference data unique to said apparatus.

11. A method as in claim 5 or 9 further comprising the step of downloading a plurality of encryption keys and encryption algorithms from said authentication center to said memory means.

12. A method of encrypting a communication session comprising the steps of:

performing the steps of claim 9;

downloading a plurality of encryption keys and encryption algorithms from said authentication center to said memory means;

receiving a message from said authentication center confirming the identity of said user; and,

encrypting the balance of the communication session using at least one of said downloaded encryption algorithms.

13. A method as in claim 12 wherein said step of encrypting the balance of said communication session comprises using encryption keys which include at least one encryption key derived from said biometric data.

14. A method as in claim 12 wherein said step of encrypting the balance of said communication session comprises using a plurality of said downloaded encryption algorithms in succession.

15. A method as in claim 12 further comprising the step of using said biometric data in the encryption process.

16. A method as in claim 15 wherein the step of encrypting the balance of said communication session comprises using at least one encryption key derived from said biometric data and at least one key not derived from said biometric data.

17. A method as in claim 16 wherein the biometrically derived key and said key not derived from biometric data are sequentially used in the encryption process and said sequence is varied throughout the communication session.

18. A method for authenticating the identity of users of communication devices comprising:

recording the identity and biometric data of a plurality of users in a database;

configuring a plurality of apparatus for encrypting biometric data and for providing such encrypted biometric data for transmission by a communication device;

receiving a communication from a communication device associated with one of said plurality of apparatus, said communication comprising encrypted biometric data of a user of said communication device;

decrypting said communication and authenticating the identity of the user; and,

transmitting the results of said step of authenticating.

19. A method as in claim 18 wherein said step of transmitting the results comprises transmitting the results to a third party.

20. A method as in claim 18 wherein said step of configuring comprises assigning to said apparatus device-specific encryption parameters.

21. A method as in claim 20 wherein said device-specific encryption parameters include an encryption key and an encryption algorithm.

22. A method as in claim 21 wherein said parameters further include device-specific reference data.

23. A method as in claim 22 further comprising the step of from time to time downloading to said plurality of apparatus at least one encryption algorithm.

24. A method as in claim 23 wherein a plurality of encryption algorithms are downloaded from time to time.

25. A method as in claim 24 further comprising the step of:

once the identity of said user has been authenticated, selecting at least one of said downloaded encryption algorithms to be used in decrypting the balance of the communication session.

26. A method as in claim 25 wherein a plurality of said downloaded encryption algorithms are used in decrypting the balance of the communication session.

27. A method as in claim 25 further comprising the step of transmitting to said apparatus an encryption key derived from information previously provided to said authentication center by said user.

28. A method of establishing an encrypted communication with a user whose identity has been authenticated, comprising the steps of:

authenticating the identity of the user using the user's biometric data by transmitting said biometric data to an authentication center, said biometric data being encrypted according to a first encryption algorithm;

once said identity has been authenticated, encrypting said communication according to at least one second encryption algorithm which is different from said first encryption algorithm.

29. A method as in claim 28 wherein the user's biometric data is used to generate the encryption key to be used in connection with said second encryption algorithm.

30. A method as in claim 28 wherein said at least one second encryption algorithm comprises a plurality of algorithms each of which is used at different stages of the communication session.

31. A method as in claim 30 wherein the user's biometric data is used to generate the encryption key to be used in connection with said second encryption algorithm.

32. A method as in claim 29 wherein said encrypted communication comprises generating data packets having a plurality of components, one of said components comprising session information supplied by said user (such as financial transaction data or spoken messages), the other of said components not comprising such session information.

33. A method as in claim 32 wherein said components of said data packets are given varying relative positions in the course of the communication session.

34. A method as in claim 32 wherein said other components comprise biometric data.

35. A method as in claim 32 wherein said other components comprise reference data specific to a device being used to conduct said encryption.

36. A method as in claim 32 wherein each of said components is encrypted using a different encryption algorithm and a different encryption key.

37. A method as in claim 30 wherein successive algorithms to be used at said different stages have previously been transmitted from said authentication center and have been stored in memory means.

38. A method as in claim 37 wherein said second encryption algorithm is retrieved from said memory means and is selected from a plurality of algorithms in said memory means according to the time said second encryption is undertaken.

39. A method as in claim 28 further comprising the step of transmitting, to apparatus being used by said user to encrypt the user end of said communication, an encryption key

derived from information previously provided by said user to said authentication center, and using said encryption key in subsequent decryption of said communication.

40. A method of encrypting a communication from a user using an encryption algorithm and an encryption key comprising the steps of:

collecting from said user biometric data which uniquely identifies said user; and,

using said biometric data as a component of said encryption key.

41. Apparatus for enabling the authentication of the user of a communication device and for encrypting a communication session comprising:

memory means for storing encryption keys and algorithms;

at least one biometric input sensor means;

an encryption engine;

a user interface; and,

processing means.

42. Apparatus as in claim 41 further comprising means for managing communications between said apparatus and a communication device.

43. Apparatus as in claim 42 wherein said user interface is incorporated into said biometric input sensor.

44. Apparatus as in claim 41 wherein said biometric input sensor means are adapted to collect data regarding at least two biometric traits.

45. Apparatus as in claim 44 wherein said biometric traits include fingerprint, voice print and pulse data.

46. Apparatus as in claim 41 or 42 further comprising a clock for determining current time.

47. Apparatus as in claim 41 or 42 wherein at least one device-specific encryption key and at least one device-specific encryption algorithm are recorded in said memory means.

48. A method of encrypting a communication session comprising the steps of:

authenticating the identity of a participant in the communication session by verifying the participant's biometric data;

previously downloading a plurality of encryption keys and encryption algorithms from said an authentication center to memory means in apparatus used to encrypt the participant's end of the communication;

encrypting the balance of the communication session using at least one of said downloaded encryption algorithms.

49. A method as in claim 48 wherein said step of encrypting the balance of said communication session comprises using encryption keys which include at least one encryption key derived from said biometric data.

50. A method as in claim 48 wherein said step of encrypting the balance of said communication session comprises using a plurality of said downloaded encryption algorithms in succession.

51. A method as in claim 48 further comprising the step of using said biometric data in the encryption process.

52. A method as in claim 51 wherein the step of encrypting the balance of said communication session comprises using at least one encryption key derived from said biometric data and at least one key not derived from said biometric data.

53. A method as in claim 52 wherein the biometrically derived key and said key not derived from biometric data are sequentially used in the encryption process and said sequence is varied throughout the communication session.

54.. A method of encrypting a communication session following authentication of the identity of a participant in said communication, said encryption using a plurality of encryption keys which collectively are a function all of the following:

the biometric traits of said participant;

a key specific to the apparatus used to encrypt the participant's end of the communication;

information provided by said participant; and,

reference data specific to the apparatus and assigned by an authentication center.

55. A method of encrypting a communication session following authentication of the identity of a participant in said communication, comprising the step of generating a plurality of data packets comprising at least two of the following components in each data packet:

encrypted biometric data;

encrypted transaction or communication data;

encrypted device reference data;

continuity check information.

56. A method as in claim 55 wherein the arrangement of said components in said data packets varies throughout the communication session

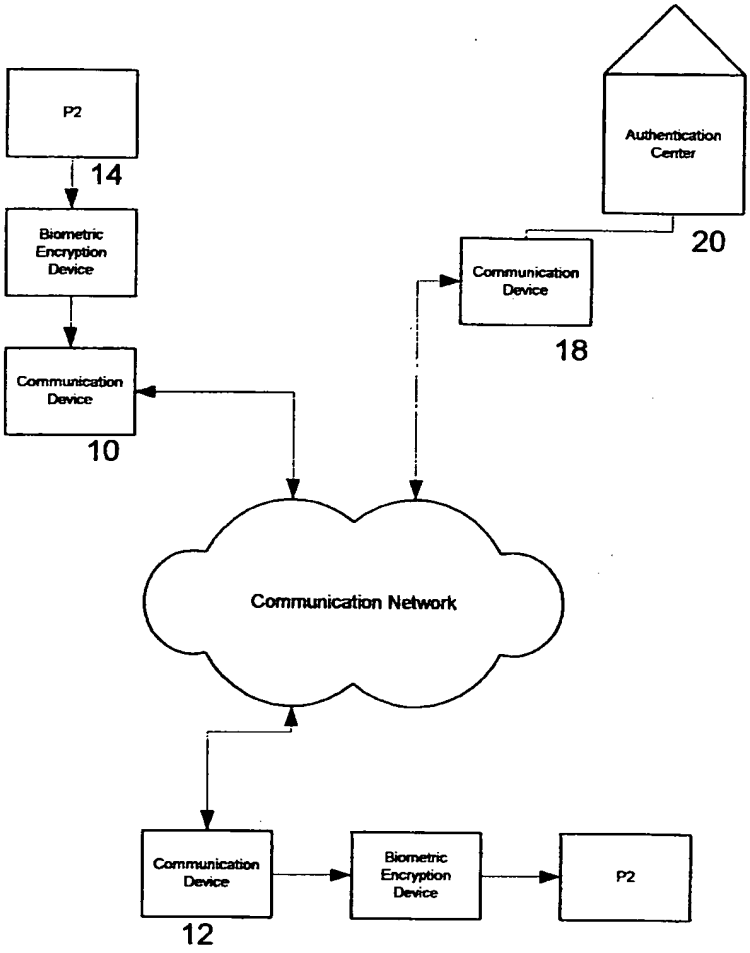

P2
14
Biometric Encryption Device
Communication Device
10
Authentication Center
20
Communication Device
18
Communication Network
Communication Device
12
Biometric Encryption Device
P2

Fig.1

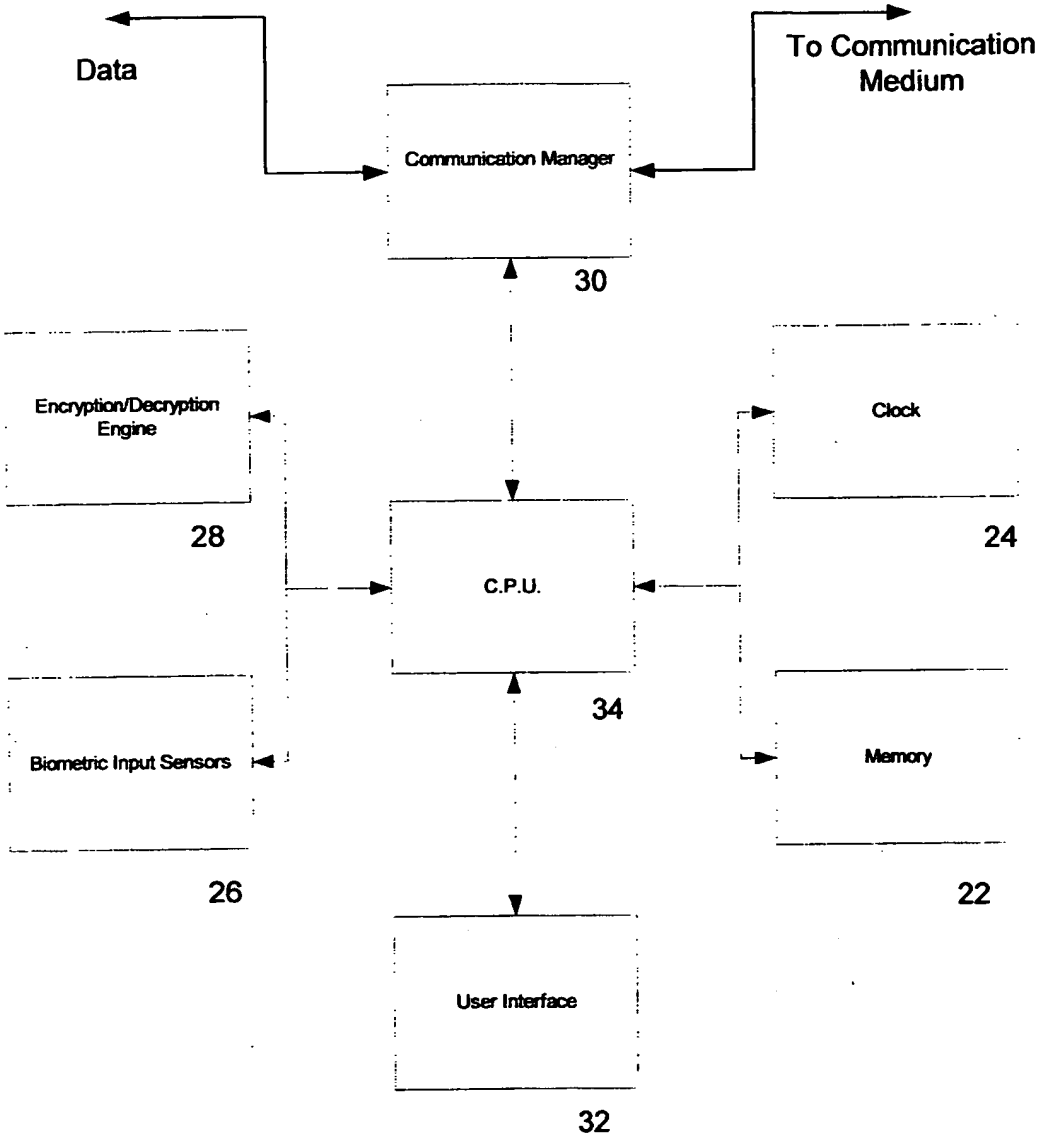

Data
To Communication Medium
Communication Manager
30
Encryption/Decryption Engine
28
Clock
24
C.P.U.
34
Biometric Input Sensors
26
Memory
22
User Interface
32

Fig.2

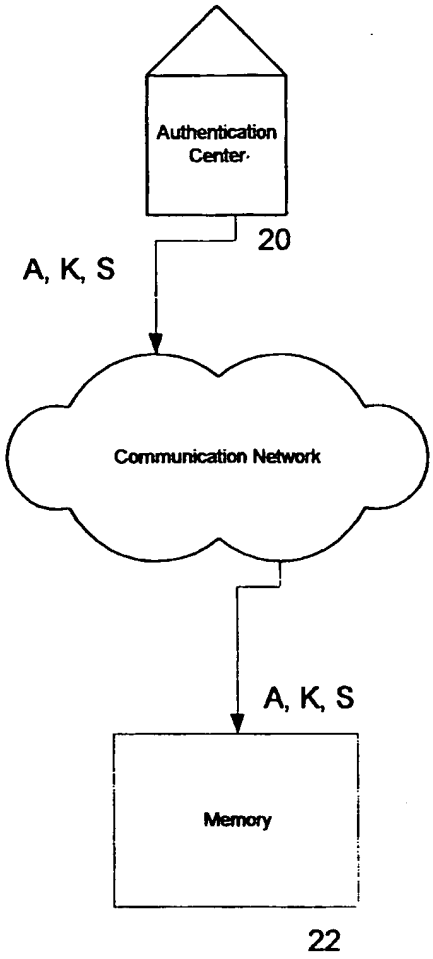

Authentication Center
20
A, K, S
Communication Network
A, K, S
Memory
22

Fig.3

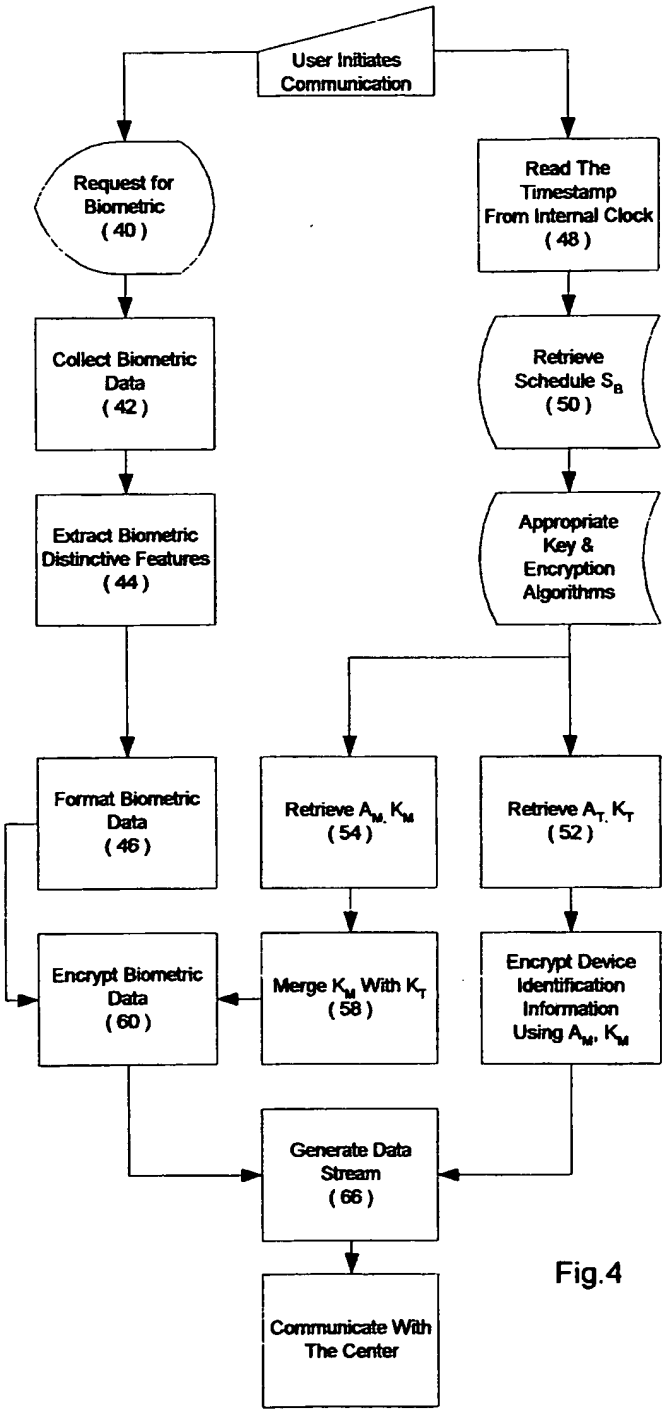

User Initiates Communication
Request for Biometric (40)
Read The Timestamp From Internal Clock (48)
Collect Biometric Data (42)
Retrieve Schedule S_B (50)
Extract Biometric Distinctive Features (44)
Appropriate Key & Encryption Algorithms
Format Biometric Data (46)
Retrieve A_M, K_M (54)
Retrieve A_T, K_T (52)
Encrypt Biometric Data (60)
Merge K_M With K_T (58)
Encrypt Device Identification Information Using A_M, K_M
Generate Data Stream (66)
Communicate With The Center

Fig.4

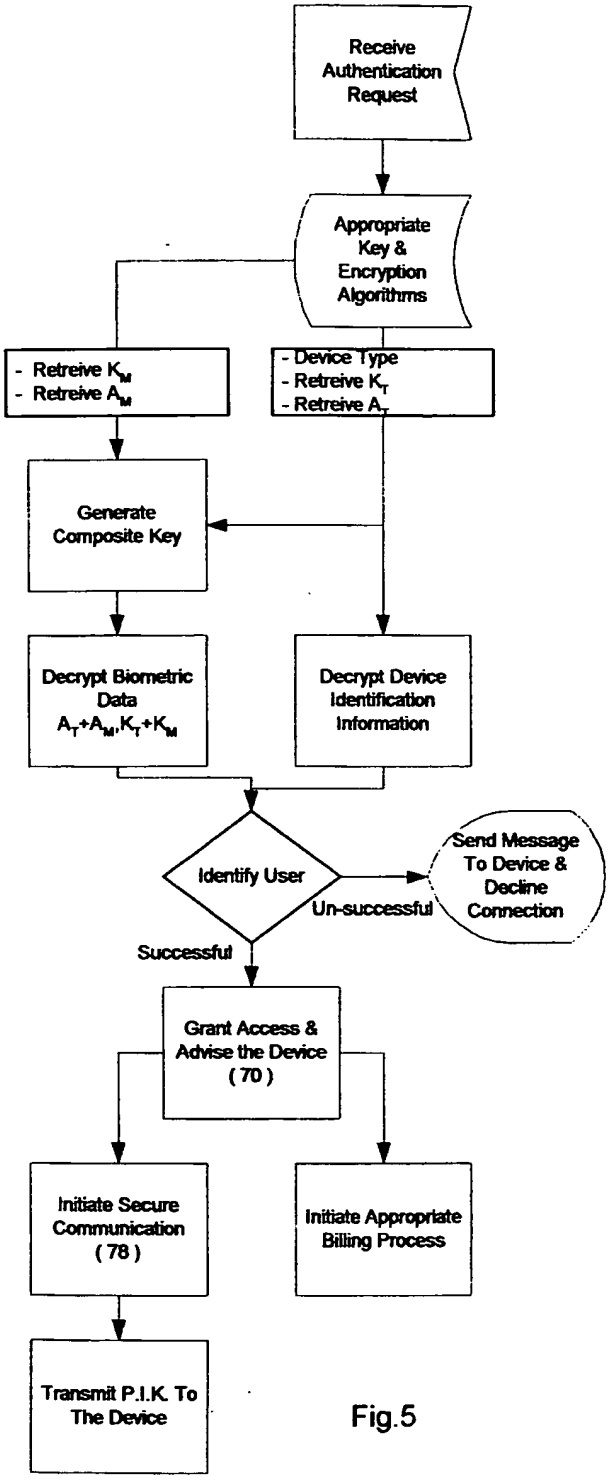

Receive Authentication Request
Appropriate Key & Encryption Algorithms
- Retreive K_M
- Retreive A_M
- Device Type
- Retreive K_T
- Retreive A_T
Generate Composite Key
Decrypt Biometric Data A_T+A_M, K_T+K_M
Decrypt Device Identification Information
Identify User
Send Message To Device & Decline Connection
Un-successful
Successful
Grant Access & Advise the Device (70)
Initiate Secure Communication (78)
Initiate Appropriate Billing Process
Transmit P.I.K. To The Device

Fig.5

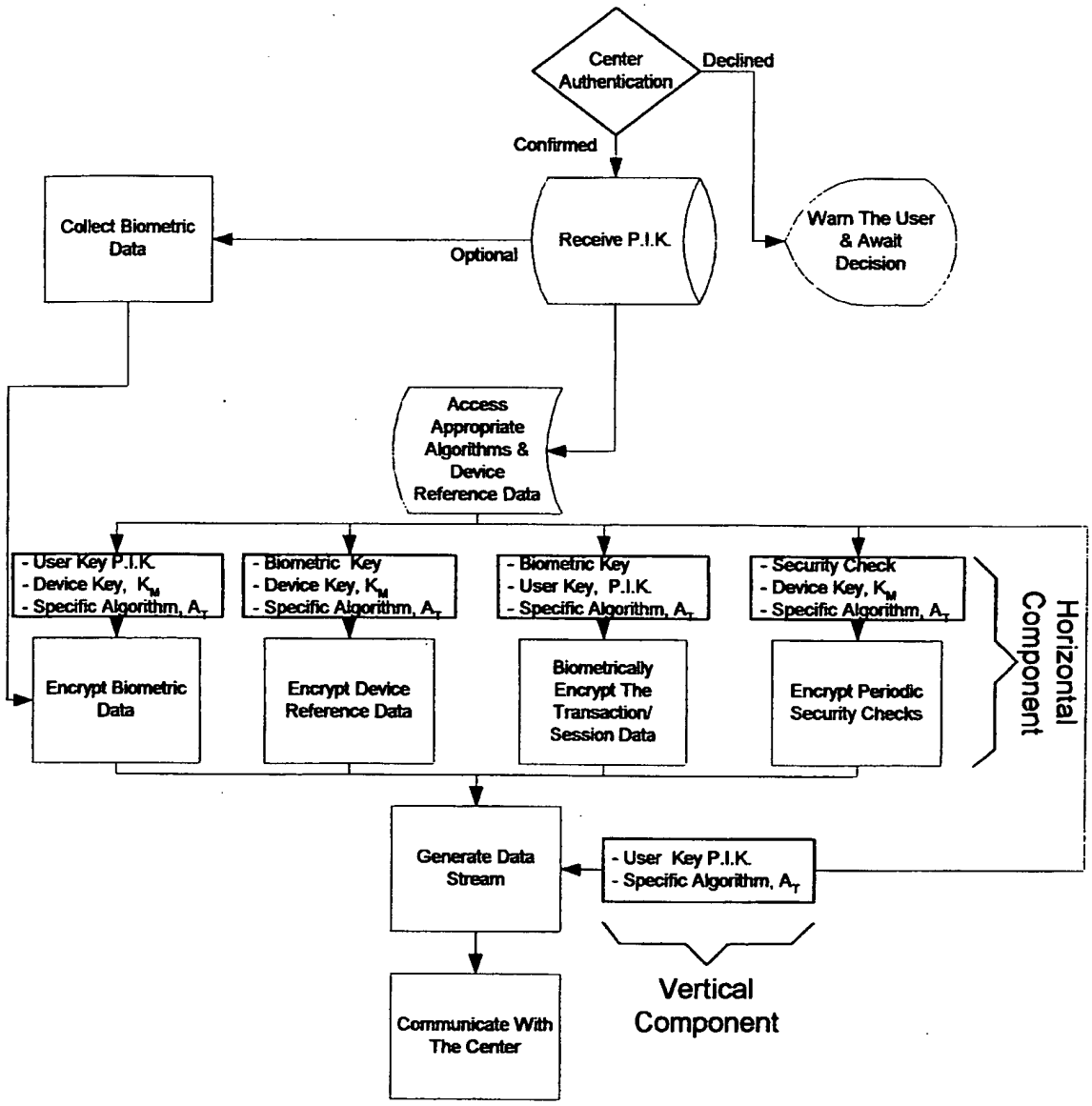

Center Authentication
Declined
Confirmed
Collect Biometric Data
Optional
Receive P.I.K.
Warn The User & Await Decision
Access Appropriate Algorithms & Device Reference Data
- User Key P.I.K.
- Device Key, K_M
- Specific Algorithm, A_T
- Biometric Key
- Device Key, K_M
- Specific Algorithm, A_T
- Biometric Key
- User Key, P.I.K.
- Specific Algorithm, A_T
- Security Check
- Device Key, K_M
- Specific Algorithm, A_T
Horizontal Component
Encrypt Biometric Data
Encrypt Device Reference Data
Biometrically Encrypt The Transaction/ Session Data
Encrypt Periodic Security Checks
Generate Data Stream
- User Key P.I.K.
- Specific Algorithm, A_T
Vertical Component
Communicate With The Center

Fig.6

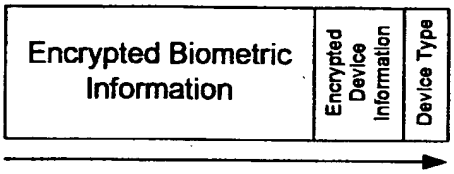

Encrypted Biometric Information
Encrypted Device Information
Device Type
Data Stream

Fig.7

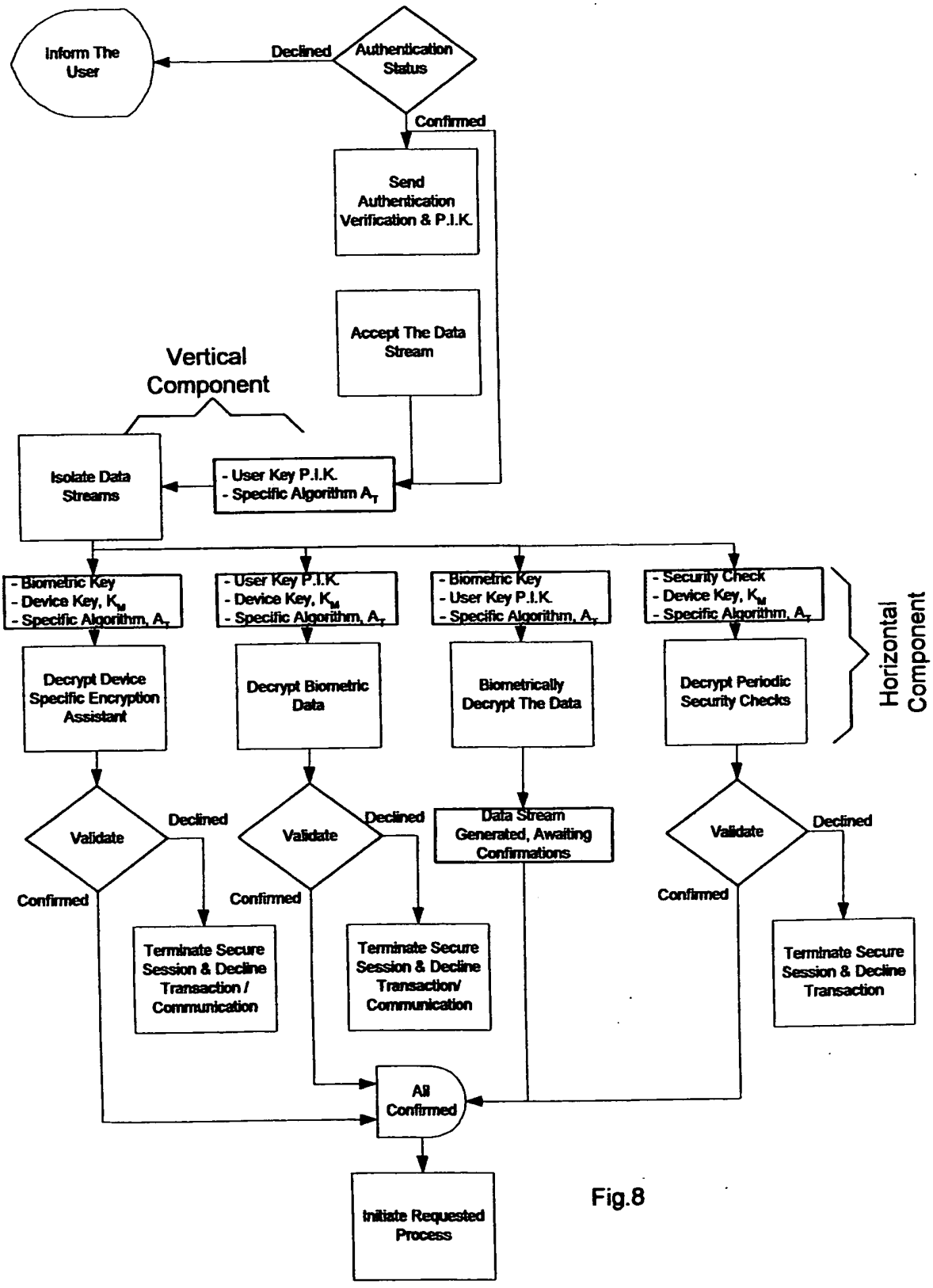

Inform The User
Declined
Authentication Status
Confirmed
Send Authentication Verification & P.I.K.
Accept The Data Stream
Vertical Component
Isolate Data Streams
- User Key P.I.K.
- Specific Algorithm A_T
- Biometric Key
- Device Key, K_M
- Specific Algorithm, A_T
- User Key P.I.K.
- Device Key, K_M
- Specific Algorithm, A_T
- Biometric Key
- User Key P.I.K.
- Specific Algorithm, A_T
- Security Check
- Device Key, K_M
- Specific Algorithm, A_T
Horizontal Component
Decrypt Device Specific Encryption Assistant
Decrypt Biometric Data
Biometrically Decrypt The Data
Decrypt Periodic Security Checks
Validate
Declined
Confirmed
Validate
Declined
Confirmed
Data Stream Generated, Awaiting Confirmations
Validate
Declined
Confirmed
Terminate Secure Session & Decline Transaction / Communication
Terminate Secure Session & Decline Transaction/ Communication
Terminate Secure Session & Decline Transaction
All Confirmed
Initiate Requested Process

Fig.8

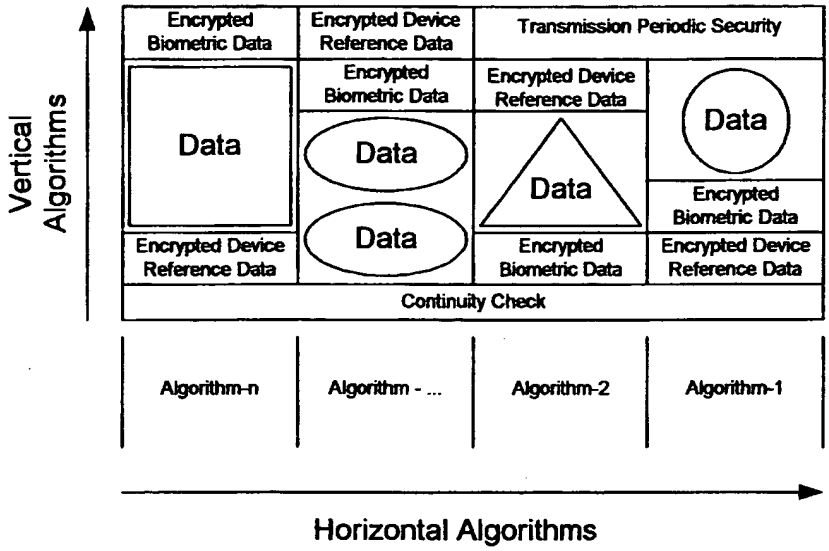

Vertical Algorithms
Encrypted Biometric Data
Encrypted Device Reference Data
Transmission Periodic Security
Data
Encrypted Biometric Data
Data
Encrypted Device Reference Data
Data
Encrypted Biometric Data
Data
Encrypted Device Reference Data
Encrypted Biometric Data
Encrypted Device Reference Data
Continuity Check
Algorithm-n
Algorithm - ...
Algorithm-2
Algorithm-1
Horizontal Algorithms

Fig.9

INTERNATIONAL SEARCH REPORT

Internat J Application No
PCT/CA 99/01164

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04L9/08

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, WPI Data, PAJ

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 5 930 804 A (YU YUAN-PIN ET AL) 27 July 1999 (1999-07-27) cited in the application	1,2,4,5, 18
A	column 2, line 43 - line 47 column 5, line 64 -column 6, line 11 column 12, line 43 -column 14, line 14	41
A	US 5 719 950 A (ARNESON MICHAEL R ET AL) 17 February 1998 (1998-02-17) cited in the application abstract column 3, line 28 -column 4, line 14	2,3,44, 45
X	DE 42 43 908 A (GAO GES AUTOMATION ORG) 30 June 1994 (1994-06-30)	40
A	column 2, line 32 - line 48 column 5, line 39 - line 54	13,15, 31,49

-/--

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
21 August 2000	28/08/2000

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Holper, G

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Interna J Application No
PCT/CA 99/01164

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No.
A	EP 0 876 026 A (MOTOROLA INC) 4 November 1998 (1998-11-04) abstract column 7, line 32 - line 50 column 10, line 41 - line 43 column 14, line 53 -column 16, line 11 column 19, line 40 - line 54	11,26,48
A	DE 44 20 970 A (ESD VERMOEGENSVERWALTUNGSGESEL) 21 December 1995 (1995-12-21) column 2, line 54 -column 3, line 24 column 4, line 21 - line 50	7-9,23
X	WO 97 25800 A (MYTEC TECHNOLOGIES INC) 17 July 1997 (1997-07-17) abstract page 7, last paragraph -page 8, last line	40,41
A	WO 97 45979 A (HITE RICHARD K ;ABRAHAM DENNIS G (US); VISA INT SERVICE ASS (US)) 4 December 1997 (1997-12-04) abstract page 11, line 18 - line 18	48,54

Form PCT/ISA/210 (continuation of second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Information on patent family members

Internal Application No
PCT/CA 99/01164

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 5930804 A	27-07-1999	EP 0923756 A	23-06-1999
		WO 9857247 A	17-12-1998
US 5719950 A	17-02-1998	AU 2186095 A	09-10-1995
		BR 9507142 A	30-09-1997
		CA 2183886 A	28-09-1995
		DE 69501327 D	05-02-1998
		DE 69501327 T	23-07-1998
		EP 0752143 A	08-01-1997
		ES 2110841 T	16-02-1998
		JP 9510636 T	28-10-1997
		WO 9526013 A	28-09-1995
DE 4243908 A	30-06-1994	NONE	
EP 0876026 A	04-11-1998	JP 10320191 A	04-12-1998
DE 4420970 A	21-12-1995	AU 3862795 A	05-01-1996
		WO 9534968 A	21-12-1995
		EP 0765550 A	02-04-1997
WO 9725800 A	17-07-1997	US 5737420 A	07-04-1998
		AU 1089597 A	01-08-1997
		US 6002770 A	14-12-1999
WO 9745979 A	04-12-1997	US 5745576 A	28-04-1998
		AU 4228197 A	05-01-1998